



INFORMATION ASSURANCE *JUST THE PARTS YOU REALLY NEED TO KNOW*

THIS BRIEF IS UNCLASSIFIED

**LtCol J. Nierle USMC
G6/Information Assurance Manager
431-2408
nierleje@mfe.usmc.mil**



What's the Purpose?



- **Know the rules**
- **Protect National Security Information and Systems**
- **Stay Out of Jail**
- **Satisfy the annual training requirement**

UNCLASSIFIED



How much do you care to know?



NIERLEJE on MFEG6L10

UNCLASSIFIED


NIPRNET

Marine Corps Information Assurance Program - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Media Print Mail

Address <http://hqusmc.hqmc.usmc.mil/c4/IA/Pages/Orders.htm> Go Links



Marines

The Few. The Proud.

RECRUITING HOMC UNITS CAREER Marine ONLINE Marine 4 Life NEWS FAMILY PUBLICATIONS LOCATOR LINKS

UNITED STATES MARINE CORPS - INFORMATION ASSURANCE PROGRAM - Official Website

Menu
[Back to C4 Home](#)
[IA Home](#)
[Policy and Guidance](#)
[Boards and Forums](#)

Information Assurance Policy and Guidance

This page provides a list of Marine Corps Information Assurance (IA) Program policy documents. These policy documents consist of Marine Corps Orders, Directives, Standards and Naval Messages like ALMARS and MARADMINs.

Other pages list higher-level references and references from other services that are commonly used within the Information Assurance Community. The higher-level references are provided as guidance while a Marine Corps specific policy is still being developed. References from other services are provided to assist in the development of policy and to provide insight when working within a joint environment.

The goal of this page is to provide you a 1-stop shop for the references you need to get your IA mission accomplished. Though some references are not linked directly, a link is provided to that reference's authoritative source.

If there are documents you feel should be listed, please suggest them to the USMC IA Branch Office at HQMCI@hqmc.usmc.mil.

Marine Corps Policy

Marine Corps Orders

The Authoritative source for Marine Corps Orders is <http://www.usmc.mil/directiv.nsf/web+orders>.

Marine Corps Order	Subject
NAVMC 2761	CATALOG OF PUBLICATIONS
MCM 2002	Manual For Courts-Martial United States (2002 Edition)

Start Policy... Inbox... TheR... Micro... Comm... Adob... Marin... untitl... 09:22

Marine Corps Information Assurance Program - Microsoft Internet Explorer

File

Edit

View

Favorites

Tools

Help

Back

Forward

Stop

Home

Search

Favorites

Media

Print

Save

Open

Close

NIERLEJE on MFEG6L10

UNCLASSIFIED

NIPRNET

Marine Corps Information Assurance Program - Microsoft Internet Explorer

File

Edit

View

Favorites

Tools

Help

Back

Forward

Stop

Home

Search

Favorites

Media

Print

Save

Open

Close

Address

http://hqusmc.hqmc.usmc.mil/c4/IA/Pages/Orders.htm

Go

Links

MCO 3430.8	Policy For Information Operations W/ Erratum
MCO 5210.11D	Records Management Program for the Marine Corps W/ CH 1 and 2
MCO 5239.2	Marine Corps Information Assurance Program
MCO 5271.1A	Information Resources Management (IRM) Standards And Guidelines Program
MCO 5271.2A	Automated Information System (AIS) Strategic Planning
MCO 5271.3C	Information Technology Steering Group Charter
MCO 5510.15A	Security Of Marine Corps Installations And Resources
MCO P5211.2B	The Privacy Act of 1974.pdf
MCO P5510.18A	United States Marine Corps Information And Personnel Security Program Manual W/ Ch 1
MCO P5530.14	Marine Corps Physical Security Program Manual
MCO 7300.22	Controlling Conference Costs

ALMAR Messages

The Authoritative source for Marine Corps ALMAR Messages is <http://www.usmc.mil/almars/almar2000.nsf/almars>

ALMAR	subject
ALMAR 365-95	Department Of The Navy (DON) Policy For Incident Response And Vulnerability Reporting
ALMAR 438-96	Computer Virus Advisory And Policy
ALMAR 025-97	Military Thinking And Decision Making Exercises
ALMAR 068-97	Marine Corps Access To The Internet Permissible

UNCLASSIFIED

NIPRNET

NIERLEJE on MFEG6L10

UNCLASSIFIED

NIPRNET

Marine Corps Information Assurance Program - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address http://hqusmc.hqmc.usmc.mil/c4/IA/Pages/Orders.htm Go Links

ALMAR 368-97	Guidance For Internet Use Publication Of Information On The World Wide Web
ALMAR 021-01	Marine Corps Information Operations (IO)
ALMAR 007-04	Operations Security (OPSEC)

Marine Corps Information Assurance Program - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address http://hqusmc.hqmc.usmc.mil/c4/IA/Pages/Orders.htm Go Links

MARADMIN Messages

The Authoritative source for Marine Corps MARADMIN Messages is
<http://www.usmc.mil/maradmins/maradmin2000.nsf/maradmins>

MARADMIN	Subject
MARADMIN 003-98	Marine Corps Disposal Policy Advisory 98-02: Disposal Process For Commercial Off-The-Shelf (COTS) Software And Automation Resources (AR) Information Technology (IT) Equipment Pursuant To The Defense Automation Resources Management Program (DARMP)
MARADMIN 083-98	Web Site Policy Review
MARADMIN 109-98	Web Site Policy Review-Revision
MARADMIN 123-98	Marine Migration To NT NOS And Exchange Messaging Systems
MARADMIN 158-98	Information Assurance Training And Certification (IAT&C)
MARADMIN 071-99	Information Assurance Training And Certification (IAT&C) Update
MARADMIN 083-99	Marine Corps Enterprise Network (MCEN) Circuit Management
MARADMIN 084-99	Marine Corps Enterprise Network (MCEN) Assurance
MARADMIN 094-99	World Wide Web Site Compliance Assessment
MARADMIN 099-99	Revocation Of Information Assurance Testing & Certification (IAT&C) Individual Reporting Procedures

UNCLASSIFIED

MARADMIN 197-99	Information Assurance Bulletin 1-99, Appropriate Use Of Marine Corps Information Resources
MARADMIN 235-99	Merger Of The United States Marine Corps Network Operations Center (USMC NOC) And The Marine Corps Computer And Telecommunications Activity (MCCTA)
MARADMIN 248-99	Marine Corps Public Key Infrastructure (PKI) Implementation Program
MARADMIN 254-99	Network Directory Update Process
MARADMIN 322-99	Coordinated Defense Of The Marine Corps Enterprise Network (MCEN)
MARADMIN 337-99	Network Security
MARADMIN 334-99	Procurement Reporting (Correction submitted by Sgt Shouse, MCRDPI)
MARADMIN 541-99	Information Assurance Bulletin 2-99, Guidance on the Use of Commercial Electronic Mail (EMAIL) Services
MARADMIN 136-00	Information Assurance Bulletin 1-00, Chain Email-Identifying Promotional And Virus Hoaxes
MARADMIN 162-00	Information Assurance Bulletin 2-00, Appropriate Use Of Government Information Technology Resources
MARADMIN 208-00	Information Assurance Bulletin Number 4-00, Issuance Of DoD Public Key Infrastructure (PKI) Server Certificates To All Private USMC Web Servers
MARADMIN 267-00	Information Technology Advisory 00-03 Marine Corps Information Technology (IT) Requirements And Acquisitions Policy
MARADMIN 424-00	Web-Based Information Technology (IT) Training Courses
MARADMIN 555-00	DoD Smart Common Access Card (CAC) Equipment Implementation
MARADMIN 628-00	Marine Corps Government-Wide Commercial Purchase Card Program (CMC Message 281000z Dec 00)

FILEJE on MFEG6L10

UNCLASSIFIED

NIPR

Marine Corps Information Assurance Program - Microsoft Internet Explorer

http://hqusmc.hqmc.usmc.mil/c4/IA/Pages/Orders.htm

Go

MARADMIN 628-00	Marine Corps Government-Wide Commercial Purchase Card Program (CMC Message 281000z Dec 00)
MARADMIN 053-01	Correction To CMC Message 281000z Dec 00 (Installing Modems To Computers Connected To MCEN Is Not Authorized.)
MARADMIN 140-01	Electronic And Information Technology Accessibility Standards
MARADMIN 329-01	Request For Applicants To Lateral Move To MOS 0689
MARADMIN 330-01	Request For Applicants To Lateral Move To MOS 0681
MARADMIN 357-01	Marine Forces Integrated Network Operations (MARFOR-INO) Name Change
MARADMIN 362-01	Common Access Card (CAC) Status
MARADMIN 375-01	Interim Policy On Appropriate Use Of Personal Electronic Devices (PEDS)
MARADMIN 390-01	Critical Infrastructure Protection (CIP) Program
MARADMIN 419-01	Selections For Lateral Move To MOS 0689
MARADMIN 439-01	Information (INFOSEC) And Operations Security (OPSEC) Reminder
MARADMIN 450-01	Marking Classified Email Messages On SIPRNET
MARADMIN 473-01	Revised Information Technology (IT) Procurement Approval Process
MARADMIN 501-01	Web Page Style Guide, New MCO 5720.26
MARADMIN 525-01	Computer Scams And Hoaxes
MARADMIN 553-01	Marine Corps Community Services (MCCS) Network Information Technology (IT) Acquisition Policy
MARADMIN 037-02	Information Technology (IT) Advisory 01-02, USMC NIPRNET And SIPRNET Software Standards
MARADMIN 038-02	Computer Network Remote Access Security

UNCLASSIFIED

Marine Corps Information Assurance Program - Microsoft Internet Explorer	
http://hqusmc.hqmc.usmc.mil/c4/IA/Pages/Orders.htm	
MARADMIN 198-02	Request For Applicants To Lateral Move To MOS 0681
MARADMIN 199-02	Request For Applicants To Lateral Move To MOS 0689
MARADMIN 200-02	MCBUL 1560. FY02 Information Assurance Scholarship Program
MARADMIN 249-02	Security Of Network Communications
MARADMIN 343-02	Change 1 To MCO P5510.18a
MARADMIN 387-02	Common Access Card (CAC) Issuance Procedures And Extension Of Issuance Deadline To Oct 2003
MARADMIN 432-02	Access To National Security Information By Non-U.S. Citizens Or Individuals Who Claim Dual Citizenship
MARADMIN 465-02	Security Of Classified Information
MARADMIN 479-02	Establishment And Implementation Of The USMC Software Baseline
MARADMIN 594-02	MCBUL 1560. FY03 Information Assurance Scholarship Program
MARADMIN 611-02	Access To Classified Information And Interim Clearance Procedures
MARADMIN 070-03	Marine Corps Community Services Information Technology Policy
MARADMIN 088-03	Electronic Spillage Of Classified Information
MARADMIN 089-03	Marine Corps Enterprise Network (MCEN) Password Management Policy
MARADMIN 201-03	Common Access Card (CAC) Policy Memo 003
MARADMIN 202-03	Marine Corps Funding Policy On Light Refreshments
MARADMIN 237-03	MCBUL 1560. Information Technology Distributed Learning Graduate Certificate Programs
MARADMIN 313-03	Establishment Of The Marine Corps Network Operations And Security Command (MCONSC)
	Information Technology Automated Data Processing Equipment (IT-ADPE)

Marine Corps Information Assurance Program - Microsoft Internet Explorer

UNCLASSIFIED

NIPP

Marine Corps Information Assurance Program - Microsoft Internet Explorer

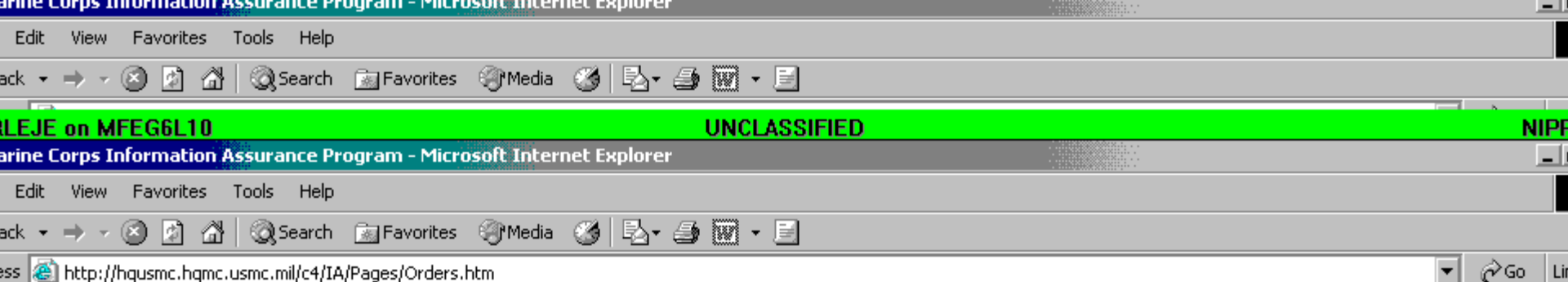
http://hqusmc.hqmc.usmc.mil/c4/IA/Pages/Orders.htm

MARADMIN 430-03	Removable Secondary Storage Media Device Policy
MARADMIN 469-03	MCBUL 1560. FY04 Information Assurance Scholarship Program
MARADMIN 476-03	Correction To Electronic Mail (E-Mail) Naming Convention Standards
MARADMIN 523-03	USMC Mainframe Terminal Emulation Client (3270)
MARADMIN 568-03	Marine Corps Enterprise Information Technology Services (MCEITS) Engineering Support
MARADMIN 581-03	The Establishment of Three Levels of Maintenance on USMC Ground Equipment
MARADMIN 598-03	Conference Costs
MARADMIN 017-04	Restructuring Department of The Navy Management of Information and Information Technology
MARADMIN 032-04	Marine Corps Internet Protocol Version 6 (IPv6) Policy
MARADMIN 047-04	Personnel Security Investigations for Instructors
MARADMIN 071-04	Unauthorized Release of Information Through Public Web Sites

Information Resource Manuals (IRMs)

The authoritative source for Marine Corps Information Resource Manuals and other technical manuals is your Unit Technical Publications Representative. An online source for Marines can be found at <http://pubs.ala.usmc.mil/>

Information Resource Manual	Title
IRM-5231-21	Automated Information System (AIS) Project Base Lining
IRM-5231-12	Automatic Data Processing Equipment (ADPE) Support Plan



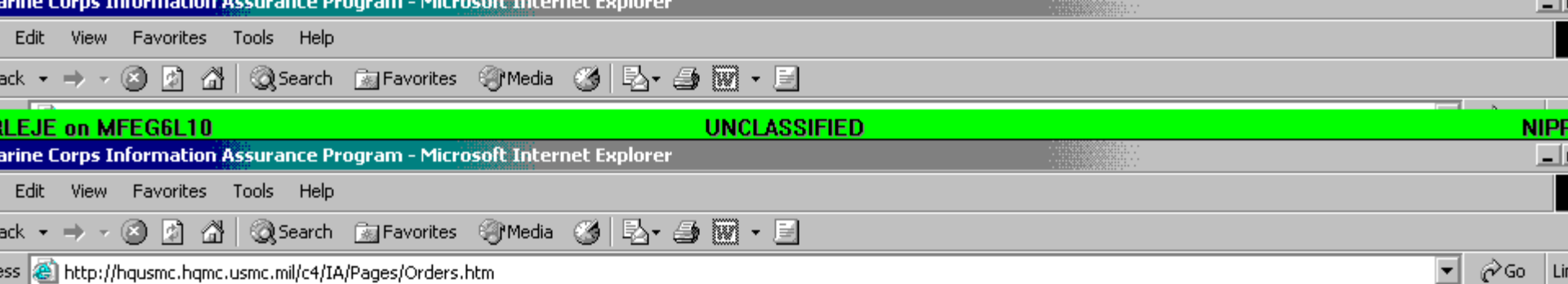
Library Management System	Network Procedures Manual
IRM-5239-01	Local and Wide Area Networks
IRM-5239-04	Telecommunications Support Plan
IRM-5239-05	Computer Security Procedures
IRM-5239-08a	Contingency Planning
IRM-5239-09	Small Computer Systems Security w/ CH1
IRM-5239-10	System Security Plan
IRM-5239-13	

Marine Corps IA Operational Standards

The Marine Corps Enterprise Network (MCEN) Designated Approval Authority (DAA) issues Marine Corps Information Assurance Operational Standards (IAOS). The IAOS series provides modules that guide the implementation of policy direction established in MCO 5239.2. The modules provide procedural, technical, administrative, and supplemental guidance for all information systems, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data within the MCEN as well as other Marine Corps information systems. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing and executing an element of the Marine Corps Information Assurance Program.

The Authoritative source for Marine Corps Operational Standards is this Site.

Marine Corps IA Operational Standards 04 August 2003	
Op Standard	UNCLASSIFIED
MC IA OPSTD 001	Incident Reporting V 1.0



The Marine Corps Enterprise Network (MCEN) Designated Approval Authority (DAA) issues Marine Corps Information Assurance Operational Standards (IAOS). The IAOS series provides modules that guide the implementation of policy direction established in MCO 5239.2. The modules provide procedural, technical, administrative, and supplemental guidance for all information systems, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data within the MCEN as well as other Marine Corps information systems. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing and executing an element of the Marine Corps Information Assurance Program.

The Authoritative source for Marine Corps Operational Standards is this Site.

Marine Corps IA Operational Standards 04 August 2003	
Op Standard	Title
MC IA OPSTD 001	Incident Reporting V 1.0
MC IA OPSTD 002	Firewalls V 1.0
MC IA OPSTD 003	Routers V 1.0
MC IA OPSTD 004	Remote Access (RAS) V 1.0
MC IA OPSTD 005	Personal Electronic Devices (PEDs) V 1.0
MC IA OPSTD 006	Virtual Private Networks (VPN) V 1.0
MC IA OPSTD 007	Privacy Access V 1.0

Think big, Start small, Scale fast

Official Marine Corps website | [Accessibility & Privacy Notice](#) | [Contact Us](#)

Command, Control, Communications and Computers

HQMC

UNCLASSIFIED



Want to look at all those?



- Visit the website yourself:
 - <http://hqusmc.hqmc.usmc.mil/c4/IA/Pages/Orders.htm>

UNCLASSIFIED



How much do you **NEED** to know?



- The right mindset: ***LEAST PRIVILEGE***
- The MFE Appropriate Use Policy
- The MFE IA order (MFEO 5239.1)
- Dos and Don'ts for practical use
- How to respond to suspected incidents
- Who to call for help

UNCLASSIFIED



“LEAST PRIVILEGE”



- You only get the access you **NEED** to accomplish your mission and tasks.
- The difference between a hacker and an IA good guy is **PERMISSION**.
 - If you don't have permission, you will be treated as a hacker.

UNCLASSIFIED



MARFOREUR

Appropriate Use Policy



- **Signed 7 April 2003**
- **Find it at H:\G-6\Information Assurance**
- **Key points:**
 - **No expectation of privacy; we can monitor anything**
 - **Violations are punishable**
 - **Personal use of govt IT must pass the test:**
 - **Is it necessary for the health, welfare, or safety reasons?**
 - **Are you sure it will not embarrass the Marine Corps?**
 - **Are you willing to share it with the Commandant?**

UNCLASSIFIED



Appropriate Use : Telephones



- **Sensitive and classified are only discussed on secure telephone lines, ie. Red Switch and STU**
 - **Be careful of background conversations**
- **Govt phones are not used by family members**
- **Red Switch is restricted to those cleared SECRET**
- **Loss of a cell phone is the same as loss of any other piece of government equipment**
- **Personal calls on cell phones are limited in the same way as personal calls from your desk.**

UNCLASSIFIED



Appropriate Use : Internet-computer



- **You MUST comply with copyright laws for software and all other material.**
 - **Freeware is generally prohibited on the govt network.**
 - **Only software you are allowed to have at home is anti-virus and personal firewall and govt created software such as PES.**
- **Access to freemail sites is prohibited from Marine Corps computers.**
- **Freemail is prohibited for official govt business regardless of where you access it from.**

UNCLASSIFIED



Appropriate Use : Expressly prohibited use



- **Accessing, storing, transmitting, displaying, distributing, processing, viewing info that is of**
 - **Pornographic**
 - **Racist**
 - **Subversive**
 - **Promotion of criminal activity incl Hate Crimes**
- **Gambling**
- **Partisan political activity**
- **Distributing or promoting religious materials**
- **Any use of govt resources for personal gain**
- **Chain letters via email**

UNCLASSIFIED



Want More?



- ***Read the entire Appropriate Use Policy***
 - *MFE appropriate use of IT_00001.PDF*

UNCLASSIFIED



IA Policy Order



- **Review of the MFE IA Policy Order Starts Here**
- **Read the whole order here:**
[**MARFOREURO P5239.1.pdf**](#)

UNCLASSIFIED



Know Your Role



- **DAA-Designated Approving Authority (Chief of Staff)**
 - Assumes all the risk for operating the system
- **IAM-Info Assurance Manager (AC/S G-6)**
 - Overall IA program manager for all systems
- **IAO- Info Assurance Officer (various)**
 - Specifically assigned for each system
- **IAT-Info Assurance Technician**
- **User**
 - *First and best line of defense*
 - ***YOU!***

UNCLASSIFIED



User Responsibilities



- ***Protect*** information and systems against threats
- ***Report*** immediately any IA incident
- ***Control*** all media and your passphrase/password/PIN
- ***Ensure*** govt systems are used only for official purpose

UNCLASSIFIED



Configuration Mgt



- **Only G-6 Marines configure computers**
- **IAM/IAO approves all changes to security settings**
- **Software is only loaded and downloaded by G-6**
- **Ditto for attachment of peripheral devices**
- **Only software on the USMC baseline is used**
- **Private software is not allowed on the MFE network**
- **Private hardware is not allowed on the MFE network**

UNCLASSIFIED



Passphrases



- **One Beer and a Haircut, Five Bucks**
 - **1Beir&ahct5\$** (number, letter, upper+lower, special symbol, at least 12 characters)
- **Don't write your passphrase down.**
- **Change it every 90 days (you have no choice)**
- **NEVER** share your passphrase with **ANYONE**
- **NEVER** share your passphrase with **ANYONE**
- **NEVER** share your passphrase with **ANYONE**

UNCLASSIFIED



Remote Access (OWA)



- **Must be from a govt computer, or a computer over which you have control (like home PC)**
 - **Must prove it has current anti-virus software**
 - **After 1 May PKI authentication will be required**
- **Prohibited from :**
 - **Libraries, Kiosks, Cyber cafes, Hotel business center**
 - **And your German girlfriend's apartment**
- **Do not underestimate the threat of eavesdropping when TAD!**
- **Don't connect a MFE computer to any network without prior approval from the IAM.**

UNCLASSIFIED



Data Access



- **Individual workstations**
 - **Data in My Documents and Desktop is only there for you**
 - **Others logged into that computer will not see that data**
- **Section Shared drives**
 - **Only members of the section have any rights**
 - **By default all members have full control**
- **HQ drives (H drive)**
 - **All MFE have full control unless you specifically change the permissions**
 - **Do NOT password protect anything on H drive; if you want to restrict access, put it on your section drive and grant permission specifically to the intended users**

UNCLASSIFIED



Data Backup



- **Shared drives**
 - Backed up by G-6 daily/weekly/monthly
- **Email and Web**
 - Same as shared drives
- **Individual workstations**
 - **Users must backup their own data on CD-R/CD-RW**
 - Request assistance from G-6 helpdesk to ensure you get all the required data

UNCLASSIFIED



NIPR to SIPR?



- **Only G-6 Helpdesk is authorized to move data from NIPR to SIPR**
- **Must be properly marked with classification on every page/slide per DoD and DoN guidance**
- **Filename must start with “(U) <filename>.<ext>”**
- **Submit a trouble ticket**

UNCLASSIFIED



SIPR to NIPR?



- High risk of ***Spillage***, so highly restricted
- Only performed by G-6 IAT or IAO
- Only these file types: .jp(e)g, .htm(l), .bmp, .gif, .txt, .rtf.
- Powerpoint is a no go.
- Submit trouble ticket and consent form (see order)
- All info must be labeled unclassified per DoD and DoN guidance

UNCLASSIFIED



SIPRNET specific regs



- Only up to SECRET or NATO SECRET
- Restrict Unclassified data on SIPRNET as it results in Hi-to-Lo transfers
- **SIPRNET passwords/phrases are SECRET and NATO SECRET so don't write them down!**
- Foreigners are not permitted access to SIPRNET
- All information on SIPR **MUST** be labeled with its classification and declass instructions, incl all email.

UNCLASSIFIED



SIPRNET EMAIL EXAMPLE

Classification: SECRET

← SIPRNET HEADER

← Overall classification of email

← DATE ORIGINATED

← Subject classification

1 May 01

Subj: (S) Subject Line must have overall and portion (U)

← Paragraph PORTION MARKING

(S) CJCSM 6510.01, CSC-STD-003-85, IA PUB-5239-26, DoD 5200.1R and SECNAVINST 5510.36 provide the marking requirements for classified AIS information and equipment.

(U) The CNO (N09N2) point of contact for this matter is Ms. Vicki Cicala

at (202) 433-8847 or email "vcicala@ncis.navy.mil".

← CLASSIFICATION/DECLAS INSTRUCTIONS

Derived from Multiple Sources
Declassify on: OLCI

← IDENTITY OF ORIGINATOR

M. Sawall
CNO (N09N2)
(202) 433-8845/DSN 288-8845

← SIPRNET FOOTER

SECRET UNCLASSIFIED

UNCLASSIFIED BUT MARKED "SECRET/NATO" FOR TRAINING PURPOSES ONLY



More complete coverage



- **For full discussion of marking of SIPR documents and email see this briefing:**
DoN-Email-Marking-Guidance-Apr03.PPT

UNCLASSIFIED



More SIPRNET regs



- **SIPR printers are SECRET; they must be in controlled areas and all output must be controlled**
 - **Mark SIPRNET output immediately with classification**
 - **Any classified SIPRNET print kept >180 days must be reported to CMCC/SCP custodians for control**
- **Switching printers between SIPR and NIPR is prohibited.**
- **NIPRNET must be separated at least one meter from SIPRNET.**

UNCLASSIFIED



NIPRNET regs



- **NIPRNET is connected to the Internet, and therefore cannot be secured. Largest threat vector to DoD.**
- **NIPRNET means “*Non-secure*” IP router network**
 - ***NO CLASSIFIED INFORMATION ON NIPRNET, EVER***
- **For Official Use Only and SBU information transmitted on NIPRNET must be encrypted**
 - **Must only use DoD PKI for encryption**

UNCLASSIFIED



Media Control



- Magnetic diskettes/discs placed into SIPRNET computers are SECRET
- Optical media placed in Read Only (CD-ROM or DVD-ROM) drives are not classified
- All media in MFE must have security classification applied: Use the Labels!
- **NEVER**, and THE ROCK means...**EVER**, place a CD or Diskette containing CLASSIFIED data into ANY NIPRNET computer or drive.

UNCLASSIFIED



Personal Electronic Devices and wireless



- **BlackBerry, cell phones, cordless phones, Palms, digital cameras, tape recorders**
- **Not allowed in the following places:**
 - **SCIF, Command Ctr, EKMS**
- **NOT USED FOR CLASSIFIED or on SIPRNET!**
 - **Exception: GSM or Iridium in SECURE mode**
- **Batteries removed when in spaces cleared for classified**
- **No synching of BlackBerry within 10 ft of SIPR!**

UNCLASSIFIED



Email, Viruses, PKI



- **Email from the Internet is the primary threat vector for viruses in DoD.**
- **Never open attachments on email that seem suspicious.**
- **Most “bad” file types are blocked: .url, .exe, etc**
- **New viruses and worms are getting better at spoofing: Do not trust originators or subject line**
- **USE PKI & only PKI. Encrypted and signed emails will not be carrying viruses**

UNCLASSIFIED



Speaking of PKI....



- **1 May 04 MarForEur OWA will require PKI authentication for access**
- **PKI encryption required for:**
 - **FOUO and SBU data transmitted on NIPRNET**
 - **Privacy data transmitted on NIPRNET (e.g. fitreps, family information, SSNs)**
- **PKI digital signature required for:**
 - **Release of DMS messages on NIPRNET**
 - **Directive emails and commitments of resources**

UNCLASSIFIED



RESPONDING TO A SUSPECTED INCIDENT



- If the email says an attachment was removed, then it is virus free, and you can just delete it.
- If you suspect the email might have a virus or that it may contain classified material:
 - **Call the G6 Helpdesk at 431-2330**
- Do NOT delete files or emails.
- Do NOT forward them to others.
- Do NOT reply to spam or suspected virus carrying email.

UNCLASSIFIED



Points of Contact



- **IAM** **LtCol J. E. Nierle, G-6, 431-2408**
- **IAO** **SSGT J. M. Rahn, G-6, 431-2187**
- **IAT** **SGT S. C. Taylor, G-6, 431-2330**
- **Helpdesk** **431-2330 or 2397**

UNCLASSIFIED



Just Bring It



-
- ✓ **Send me an email stating you completed the training: <mailto:nierleje@mfe.usmc.mil>**
 - ✓ **Print and sign this document: [MFE User Responsibility Agreement.doc](#)**
 - ✓ **Bring it to the G6 Helpdesk**
 - ✓ **Have a nice IA day.**

UNCLASSIFIED